An Information Security Evaluation Indices for an enterprise organization

Il Seok Ko*, Gwang Uk Ko**, Dae Kyung Na***, Heui Seong Na****
*Dept. of e-Commerce, Chungbuk Provincial University, isko@ctech.ac.kr
**Kumwang Technical High School
***Dept. of Economics, Sejong University
****Dept. of Computer Science, Chungbuk National University

Abstract

Most of the evaluation systems have performed evaluation with an emphasis on information security products so far. However, evaluating information security level for an enterprise needs analysis of the whole enterprise organization, and a synthetic and systematic evaluation system based on it. This study has tried to grasp the information security level of the whole enterprise organization, and develop an evaluation system of information security level for suggesting a more developing direction of information security.

1. Introduction

The importance of information security has been increasing while the whole society has become rapidly information-oriented. Information security has got to be comprehensively considered all over the organization, not limited to an information system or its technology. Also, the higher the dependence of an enterprise on information processing, the higher the loss caused by the imperfect security countermeasure of an information system[1,2]. In order to effectively achieve the object of information security of an organization, there should be criteria or evaluation models showing a direction to exactly evaluate the information security level of the whole organization, and improve it. Also, for this, there should be evaluation indices capable of evaluating and improving information security levels by sections[3,4]. The security of an enterprise should be based on analysis of the whole enterprise organization. The whole security of an enterprise organization can't be achieved only by combination of individual security products, and the information security of an organization can be effectively maintained only when the whole security & management system works well by proper union of security products/system and managerial security countermeasures. Also, the whole security level of an organization should be evaluated through proper embodiment and operation of security policy derived from operation environment and security requirements peculiar to the organization.

In order to overcome the limits of the existing researches, the study has subdivided information security elements into 5 levels - planning, environment, support, technology, and management, and developed indices based on them, and finally, made the information security level of the whole enterprise organization possible to be measured. Applying the results of the study makes possible synthetic and systematic evaluation of the information security level of an enterprise.

2. An Information Security Index System

2.1 Information Security Planning Level

The index items of information security level are composed of security policy and security plan. Security policy evaluates the general items related to information security policy. The index items of information security policy evaluate whether to establish information security policy, whether to examine and evaluate them, and the documented

part of information security policy. The indices of security plan index items also evaluate information security plan and information security investment, including items for evaluating by CSFs the essential success elements of information security environment level.

Table 1 Index System of Information Planning Level

Information security planning level	
Information security policy	Security plan
- Establishing information security policy or not / - Verifying information security policy/ - Evaluating information security policy / - Reflecting the importance of information security / - Stating information security - Verifying, and evaluating information security policy documents - Checking technological observance / - Observing security policy - Establishing action guide / - Establishing accident-settling procedure / - Stating exceptions / - Managing information and assets / - Drawing up the written oath of related manpower / - Observing information security policy - Security policy documents	- Applied-technology development investment amount - Basic-technology development investment amount - Information security investment expense - Information security plan investment amount - Drawing up a security plan

Table 2 A Information Security Environment Level Index System

Information security environment level		
Equipment security	Personnel security	
	Organizational security	Human security
- Admission-ticket management - Automatic locking device / - Facilities security / - Network management - Equipment security / - Tangible assets - Intangible assets / - Material availability security - Equipment security	- Operating an information security committee - The existence of business alternation policy - Organization management - Organizational security - Security organization - Selecting those in charge of equipment, and assigning responsibility	- Duty definition and resource allocation security - Coping with security accidents and errors - Personnel management - Human security - Licensor management

2.2 Information Security Environment Level

The index items of information security environment level are composed of equipment security and personnel security as in table 2. Equipment security evaluates the items of information security facilities and basic equipment environment as in equipment control and facilities security.

Table 3 Information Security Support Level Index System

Information security support level		
Support organization	Support activity	
Support activity	Emergency countermeasure	Education training
- Development and support process security - Plant/support equipment - Development and support process security - Appointing those in charge of information security - Stating the roles of those in charge of information security - Unification/adjustment of information security activity	- Establishing a emergency-settling plan or not - Agreements against emergency - Obstacle restoration - Settling preservation accidents and	- Education operation - Education organization - Education content - The selection method of educatees - The yearly mean number of education days
- Security-related license level	errors - Backup and restoration - Settling preservation accidents and function obstacles	- User education training - Education/training - User education/training

2.3 Information Security Support Level

The index items of information security support level are composed of support organization and support activity as in Table 3. Organization management evaluates development and support process security, appointment of those in charge of information security and their roles, security-related license level, etc; organization operation evaluates its whole matters like information activity unification/adjustment, etc.; outsourcing evaluates its own rate and sphere.

Table 4 Information Security Technology Index System

Information security technology level	
Access control operation	System function
- Access authority control / - Access control function - N/W access control / - Outsider access security - Operation system access control / - User access management - Application access control / - Network access control - Physical access security / - User approach management - User responsibility / - Network access control / - Operation system access control / - Applied-system access control / - System access and use supervision	- Account and password management - Applied-system security - Software security / - Authentication technique - Obstacle restoration / - Virus prevention - Encryption function / - Key management - The backup management of important files

2.4 Information Security Technology Level

The index items of information security technology level are divided into access control operation and system function as in table 4. The index items of access control operation are composed of indices evaluating the whole information security technology level. The index items of system function level are composed of indices evaluating the functional side (necessary to access control) and general items (on the whole account management and password).

2.5 Information Security Management Level

The indices system of information security management level, as in Table 5, is recomposed of management process requirements, documentation requirements, and BS7799 on the index items of managerial information security

management control.

Table 5 Information Security Management Level Index System

Index items	Indices	Index items	Indices
Information security policies	Approval and announcement of policy The system of policy Maintenance and management of policy an organizational system Responsibility and roles	Human security	Establishing a education and training program Enforcement and evaluation Responsibility assignation and stipulation Managing a qualification test and those in charge of major duties Secret-keeping
Transaction security	A written exchange agreement Electronic-transaction security management Electronic mail The security management of open server User official announcement	Operation management	Operation procedure and responsibility System operation Network operation Media and document management Virulent software control Establishing a business continuity management system Establishing and embodying a business continuity plan Planning, testing, maintaining and managing business continuity Mobile computing and remote working Information-asset investigation and responsibility assignation Information-asset classification and treatment
Access control	Cipher policy Cipher use Key management Access control policy User access management Access control scope		
Security-accident management	Countermeasure plan and system Countermeasure and restoration Post management	Outsider security	Contract and service level agreement security management Outsider security practice management
verification monitoring, and inspection	Observing and verifying legal requirements Observing and verifying information security policy Monitoring Security Inspection	Physical security	Physical security measures Data- center security Equipment security Office security Analysis and design security management Embodiment and performance security management Change management

2.6 Comparison with the Existing Methods

Table 6 has compared the proposed method with the existing evaluation systems. TCSEC emphasizes secrecy, of information security elements, and is hard to apply to an enterprise organization. ITSEC evaluates all information security products, with a single criterion based, and performs evaluation of products as a security guarantee part. Also, these two have evaluation objects limited to products and a system, and have common features of emphasizing each country's traits and functional elements. BS7799 is authentication of a management system; therefore, it is hard to evaluate the function of a system and the whole enterprise. Each of the existing three evaluation systems is possible to use complementarily. The system proposed by the study has subdivided each evaluation element into 5 spheres through complementation and extension of these systems; accordingly, made possible the information security level evaluation of the whole enterprise organization.

Table 6 Comparison of the evaluation systems.

Items	TCSEC	ITSEC	BS7799	Proposed method
Features	- Emphasizing secrecy, of information security elements. - Hard to apply to an enterprise organization - Limiting the object of evaluation to products and a system - Emphasizing each country's traits and functional elements	- Evaluating all information security products with a single criterion based - Performing evaluation of a product as a security guarantee part - Limiting the object of evaluation to products and a system - Emphasizing each country's traits and functional elements	- Authentication of a management system - No authentication of a product - Not enough to evaluate system function - Hard to evaluate the whole information security of an enterprise	- Possible to evaluate the information security level of the whole enterprise organization - Possible to evaluate a management system - Possible to evaluate products and a system - Subdividing each evaluation element into 5 levels

4. Conclusion

The study has divided information security elements of the whole enterprise into 5 levels to overcome the limits of the existing studies, developed indices that are based on them, and so, made the information security level of the whole enterprise organization possible to be measured. Applying the results of the study has made the information security level of an enterprise possible to be evaluated synthetically and systematically. Also, applying the evaluation methods of information security level can have evaluation progress objectively. Establishing evaluation items considering features by industry and complementing the methods could maximize the effect.

References

[1] Common Criteria Project (1998), common criteria for information technology security evaluation, common criteria

[2] B. Guptill, C. Price (1996), a security framework for enterprise using the internet, Gartner Group

[3] NIST (1995), an introduction to computer security : the NIST handbook, NIST(national institute of standards and technology)

[4] Robin Moses (1995), corporate risk analysis and management strategies, European convention on security and detection, conference publication No. 408